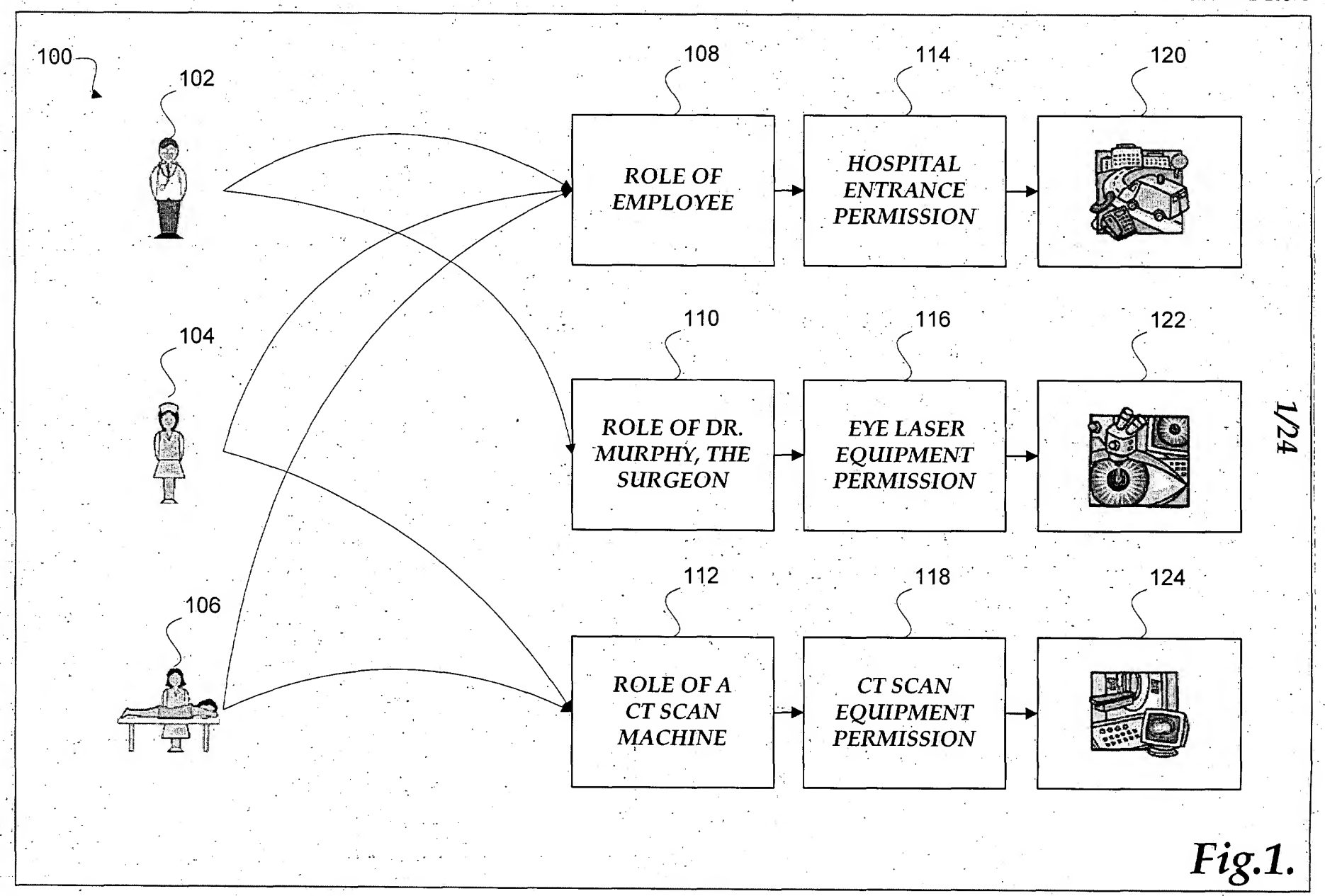


1/24

Fig.1.

Title: DISTRIBUTED EXPRESSION-BASED ACCESS CONTROL
Inventor: Shawn Oberst
Docket No.: MSFT120575

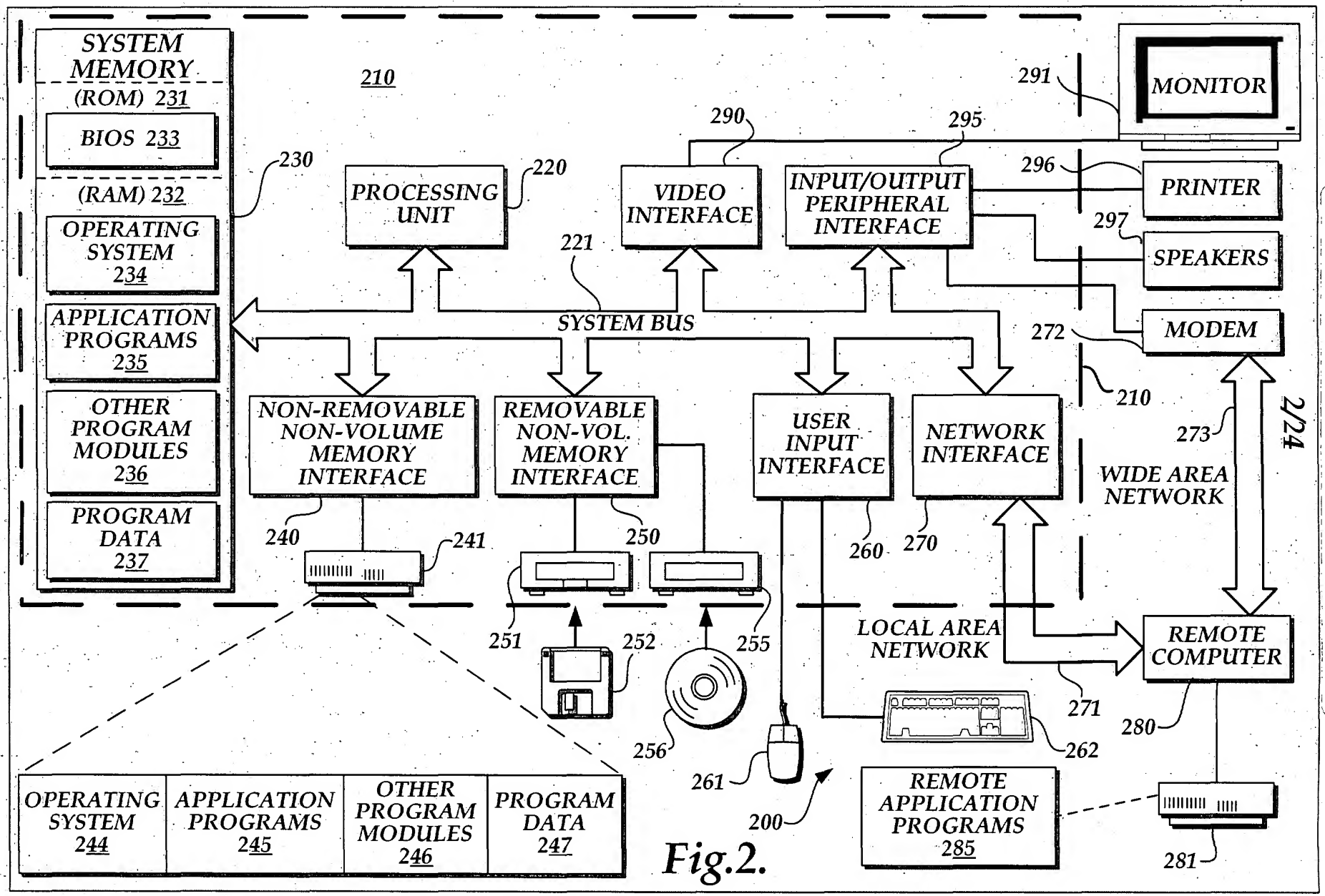


Fig.2.

2/24

DRAFT

Title: DISTRIBUTED EXPRESSION-BASED ACCESS CONTROL
Inventor: Shawn Oberst
Docket No.: MSFT120575

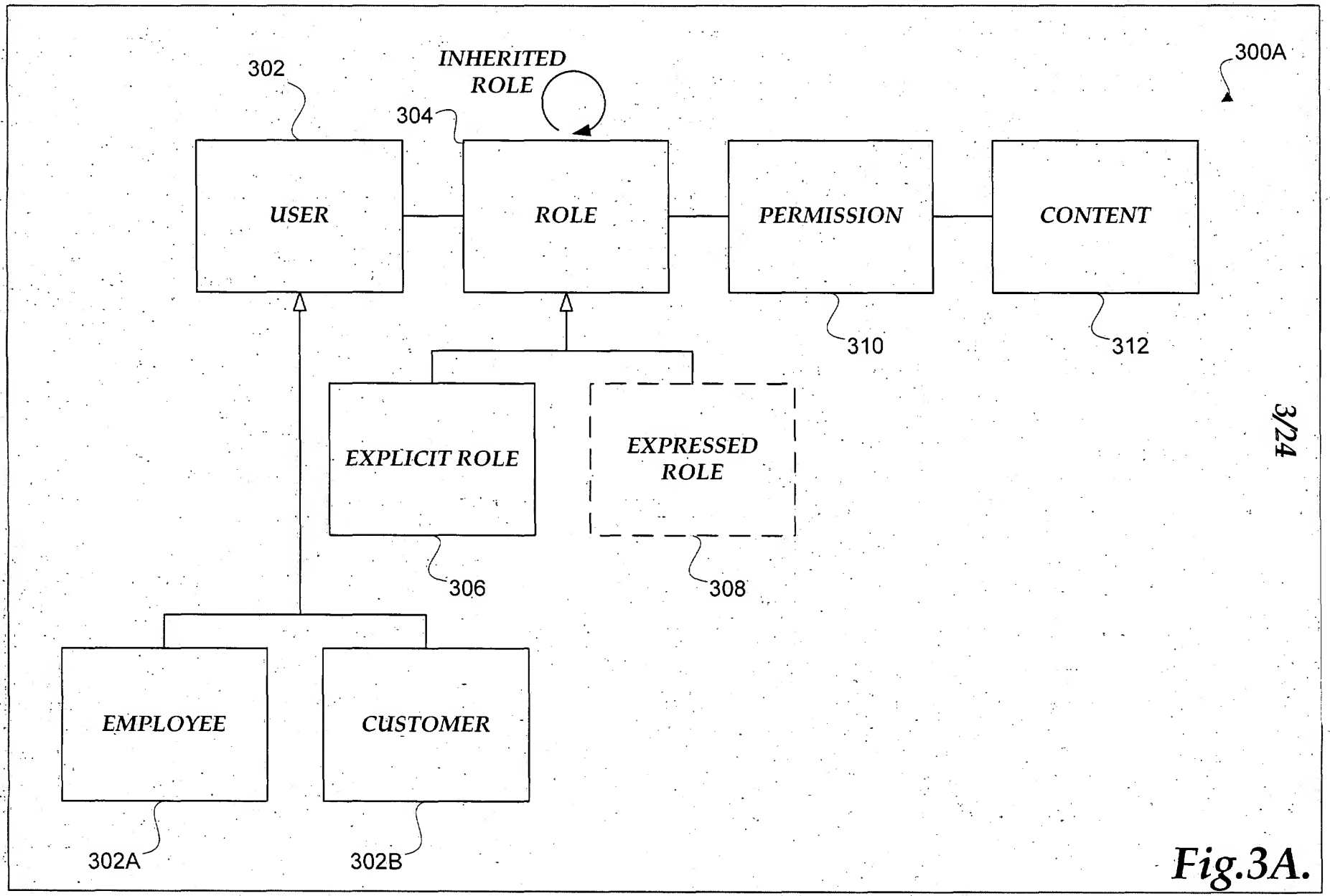


Fig.3A.

Title: DISTRIBUTED EXPRESSION-BASED ACCESS CONTROL
Inventor: Shawn Oberst
Docket No.: MSFT120575

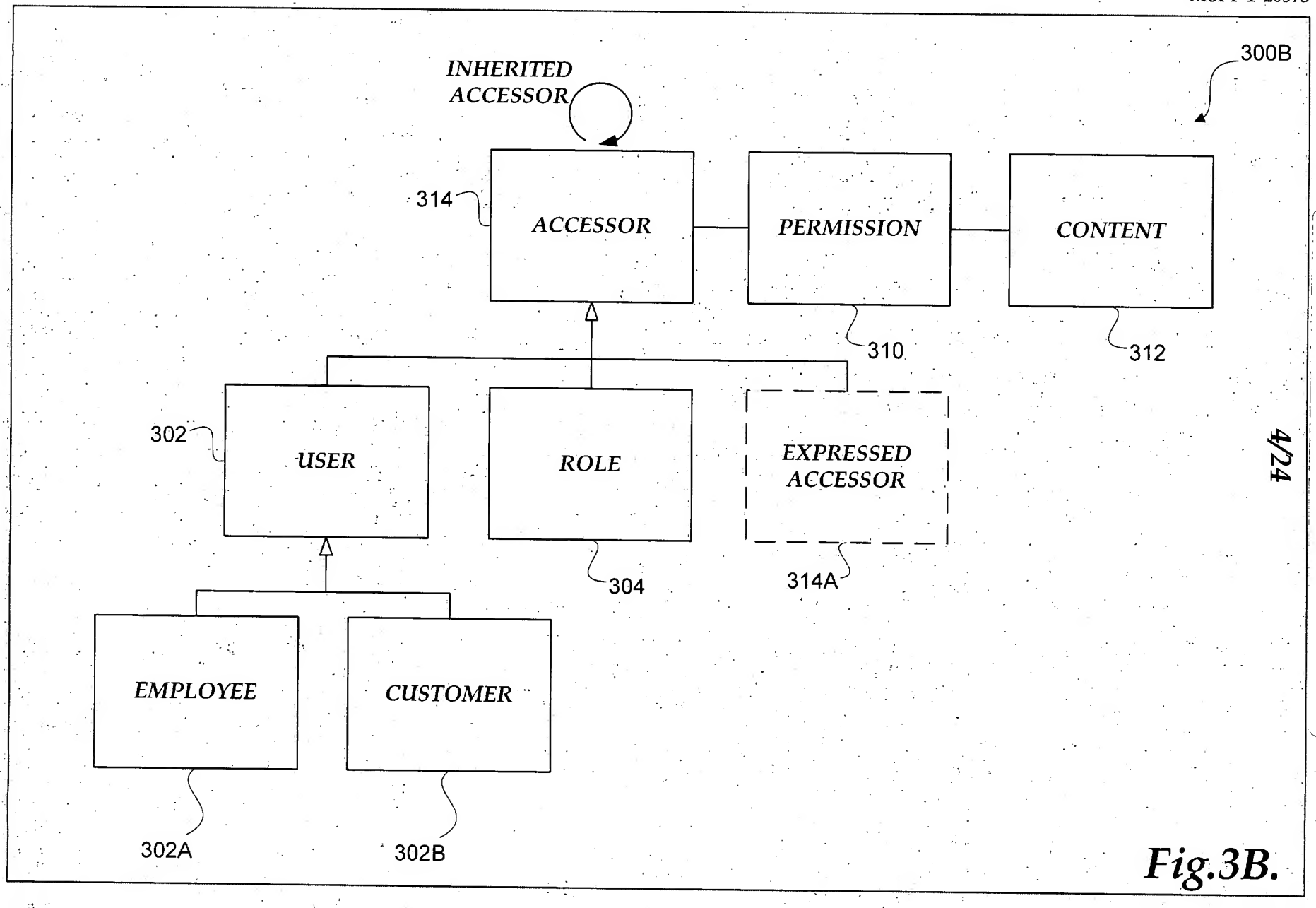


Fig.3B.

Title: DISTRIBUTED EXPRESSION-BASED ACCESS CONTROL
Inventor: Shawn Oberst
Docket No.: MSFT120575

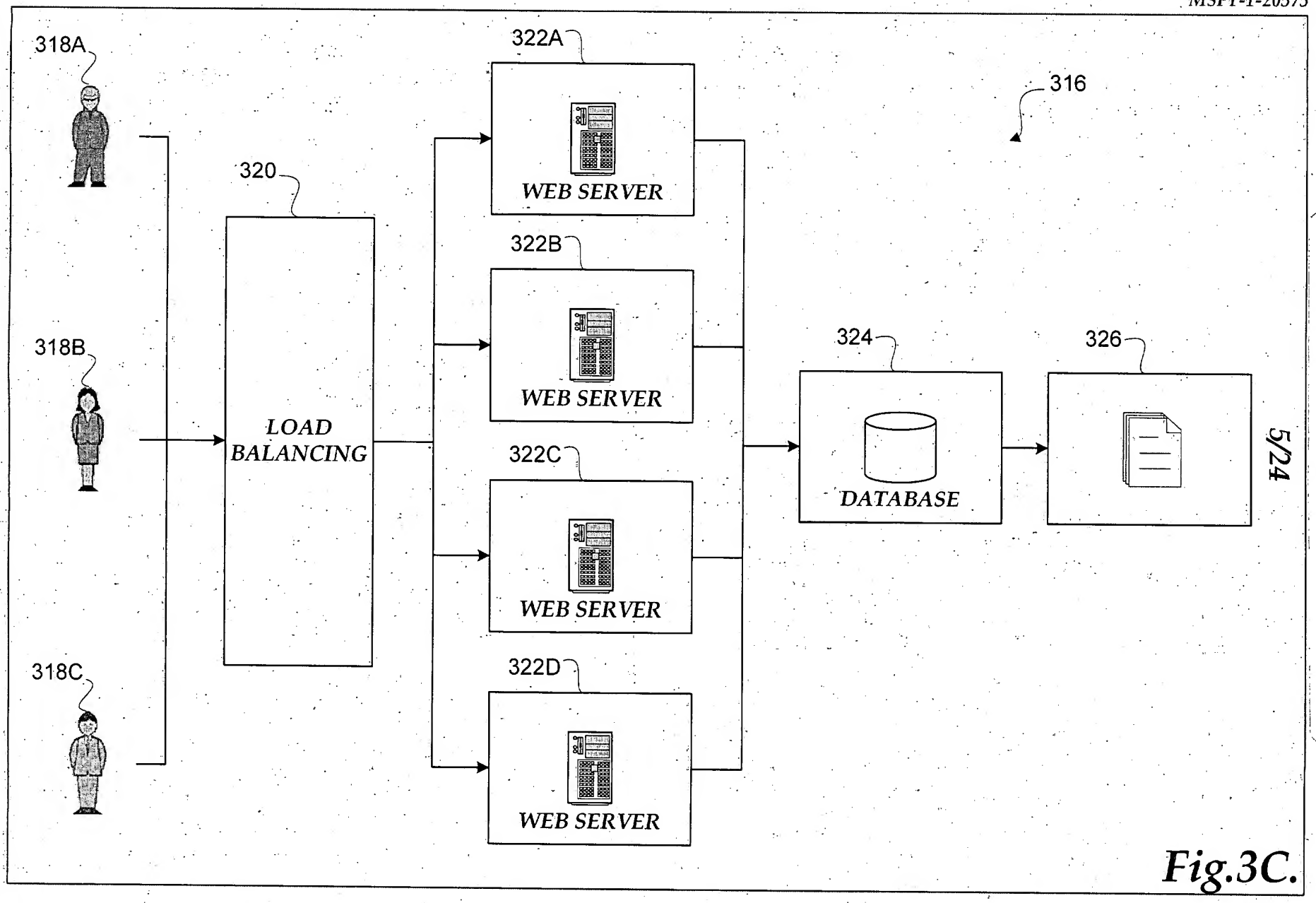


Fig.3C.

Title: DISTRIBUTED EXPRESSION-BASED ACCESS CONTROL
Inventor: Shawn Oberst
Docket No.: MSFT120575

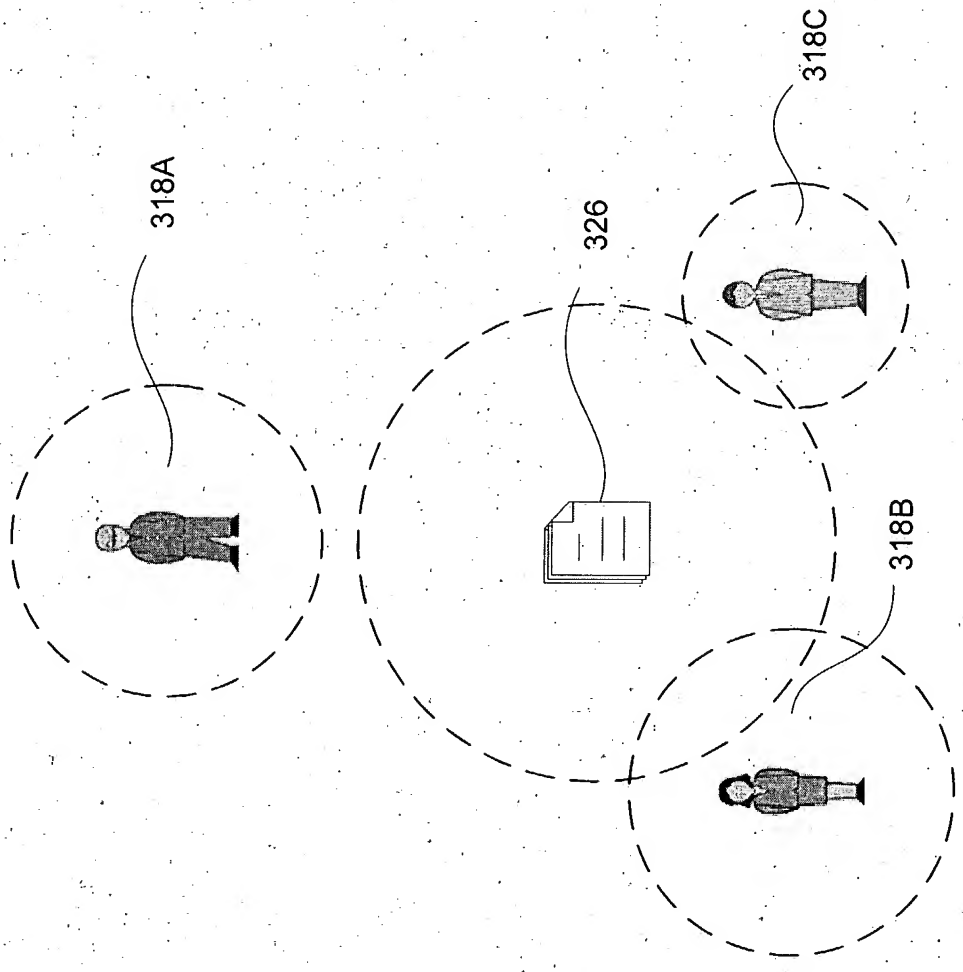


Fig.3D.

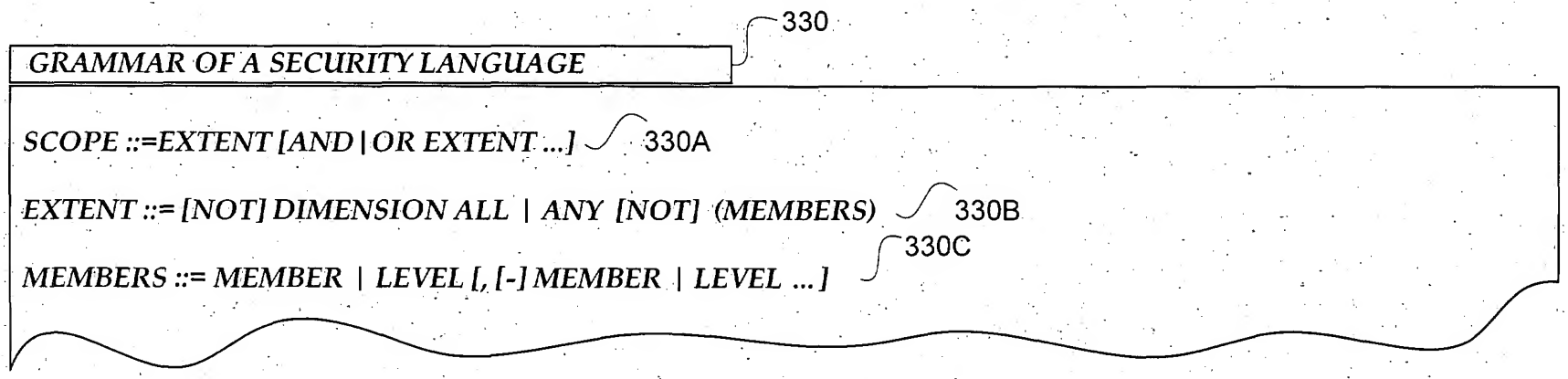


Fig.3E.

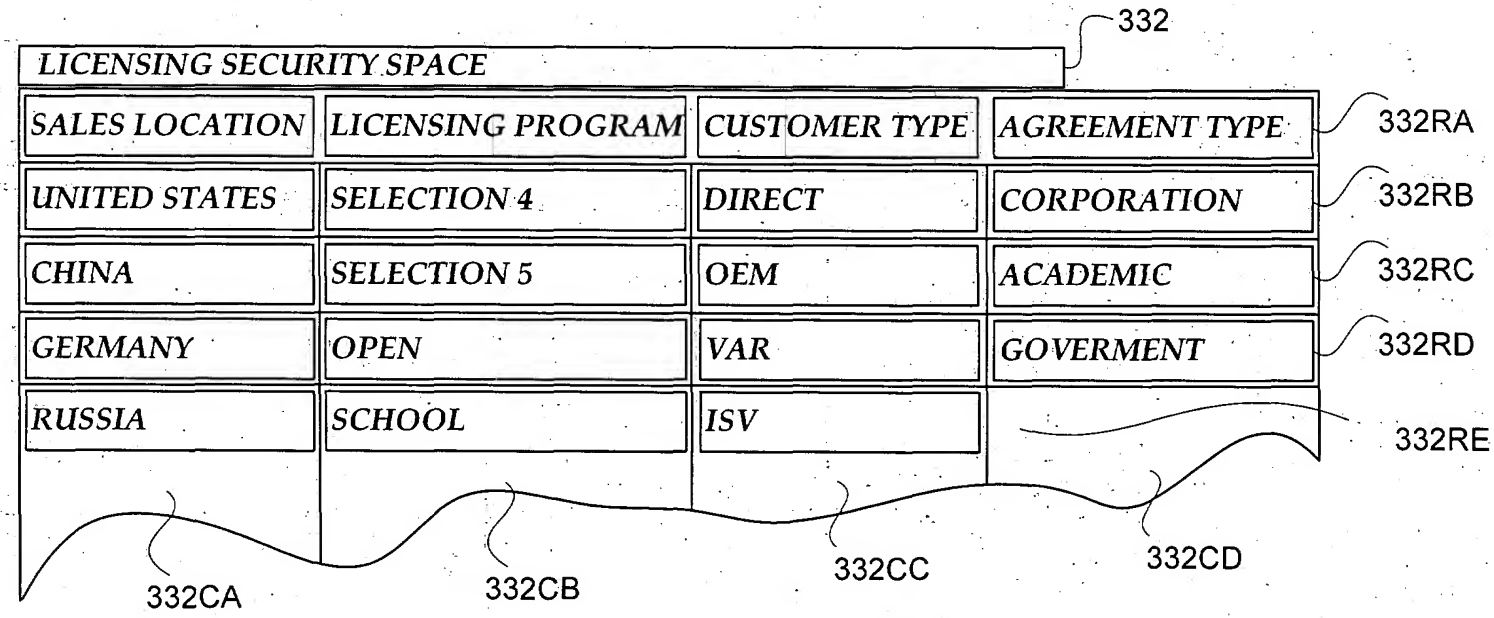


Fig.3F.

Title: DISTRIBUTED EXPRESSION-BASED ACCESS CONTROL
Inventor: Shawn Oberst
Docket No.: MSFT120575

DRAFT

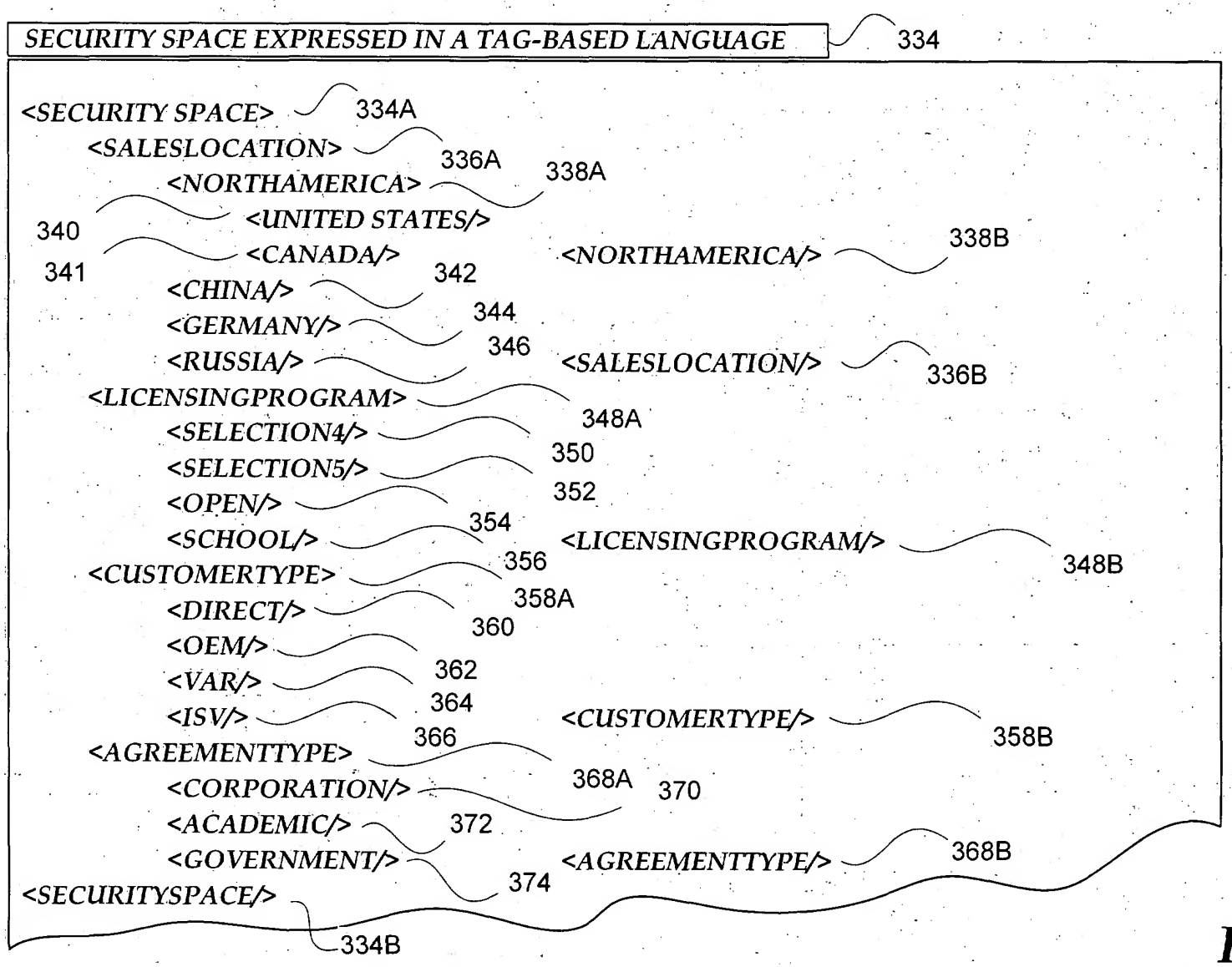


Fig.3G.

8/24

Title: DISTRIBUTED EXPRESSION-BASED ACCESS CONTROL
Inventor: Shawn Oberst
Docket No.: MSFT120575

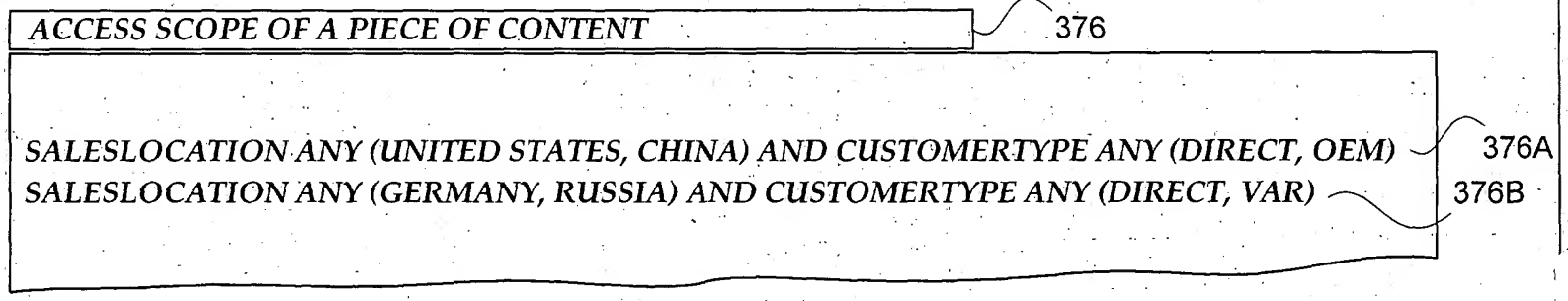


Fig.3H.

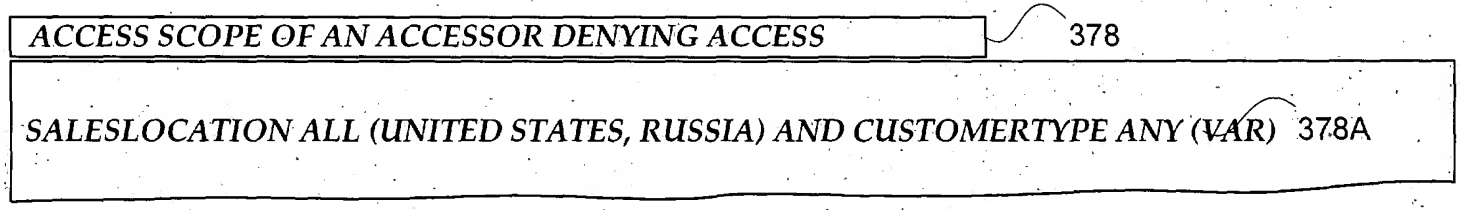


Fig.3I.

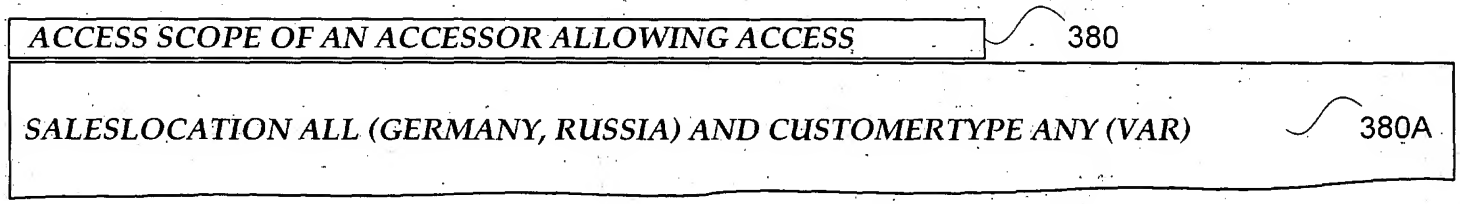


Fig.3J.

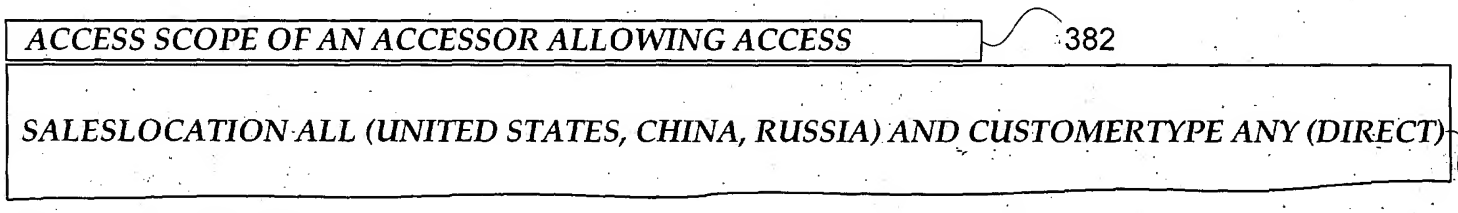


Fig.3K.

DRAFT

Title: DISTRIBUTED EXPRESSION-BASED ACCESS CONTROL
Inventor: Shawn Oberst
Docket No.: MSFT120575

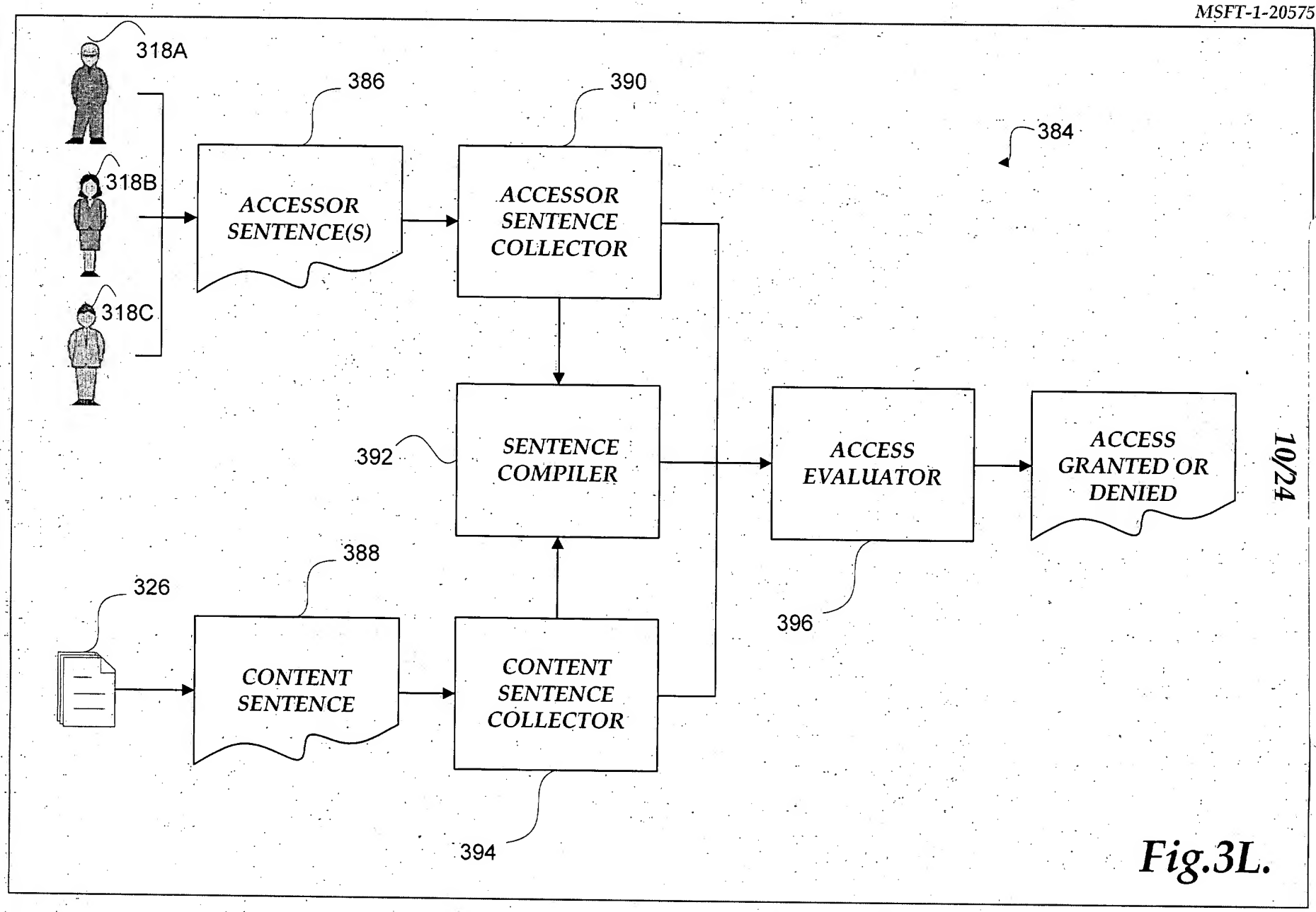


Fig.3L.

DRAFT

Title: DISTRIBUTED EXPRESSION-BASED ACCESS CONTROL
Inventor: Shawn Oberst
Docket No.: MSFT120575

Fig.3M.

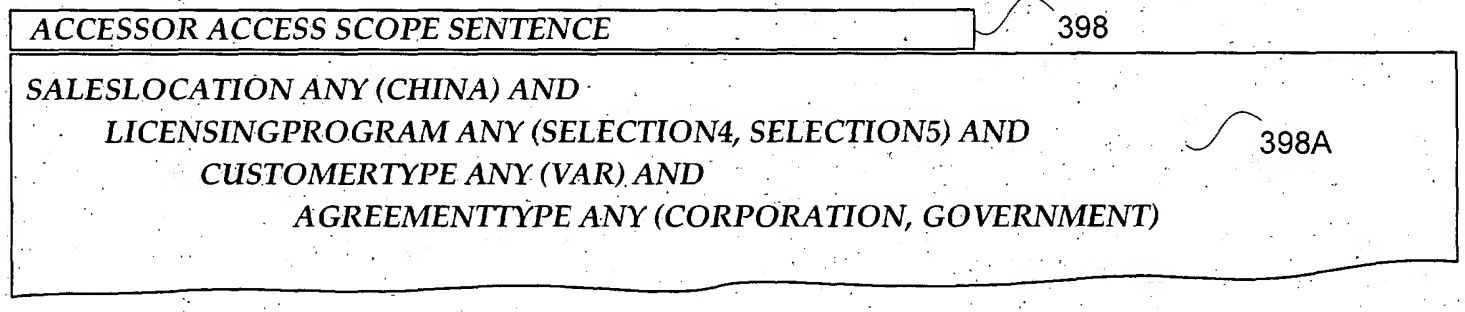


Fig.3N.

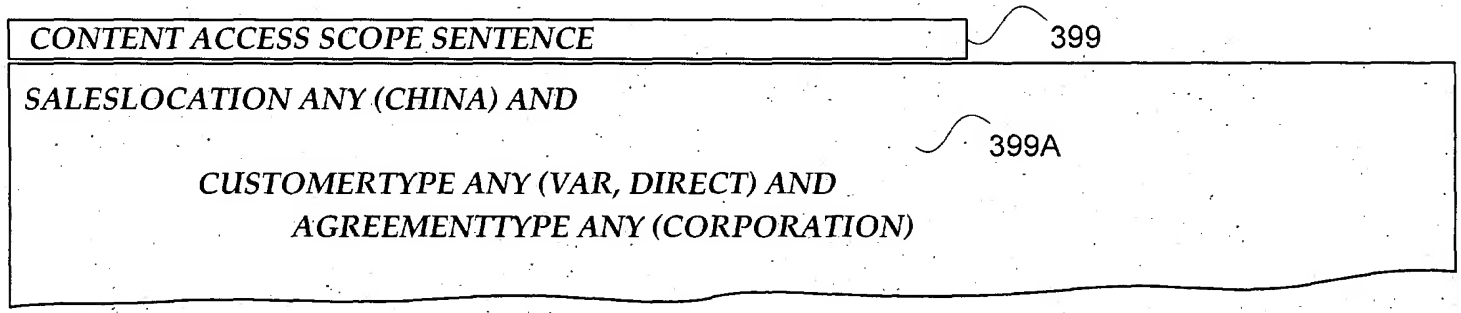
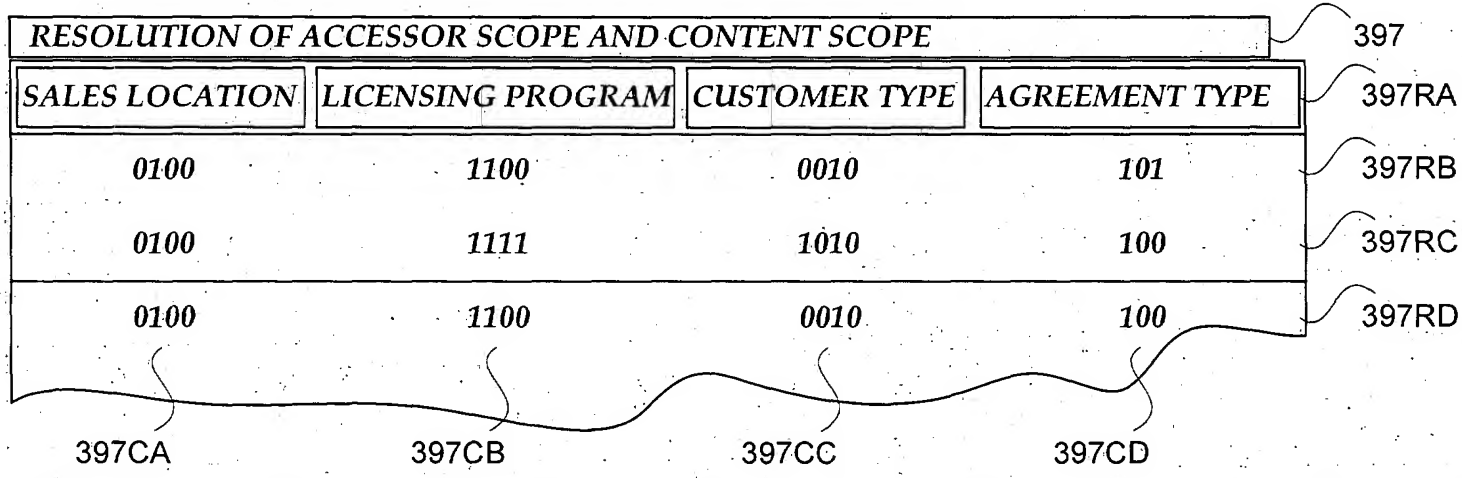


Fig.3O.



DRAFT

Title: DISTRIBUTED EXPRESSION-BASED ACCESS CONTROL
Inventor: Shawn Oberst
Docket No.: MSFT120575

Fig.3P.

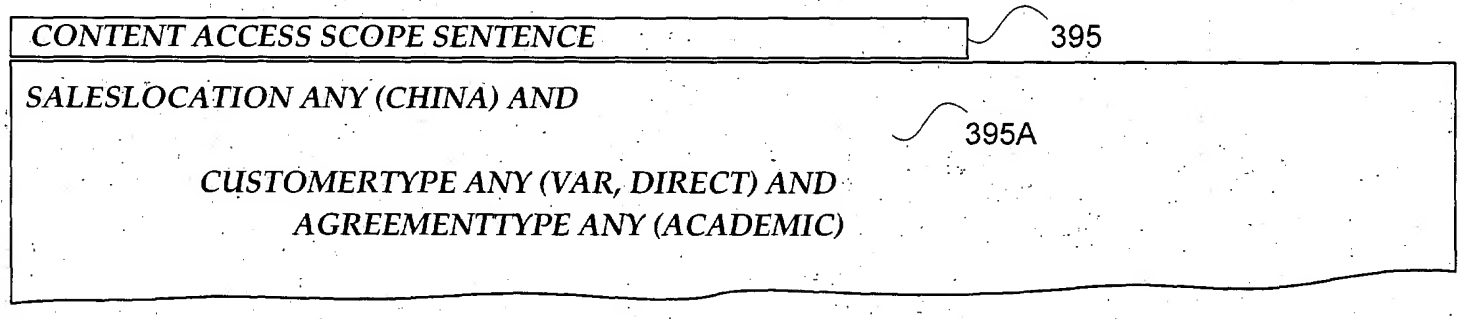
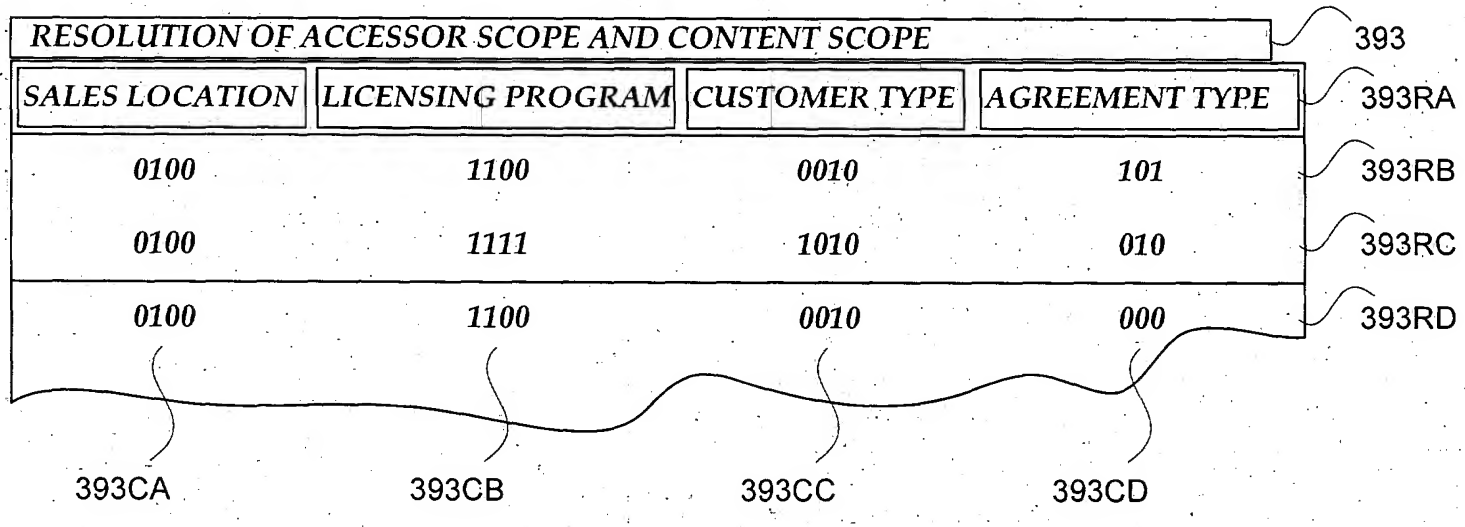
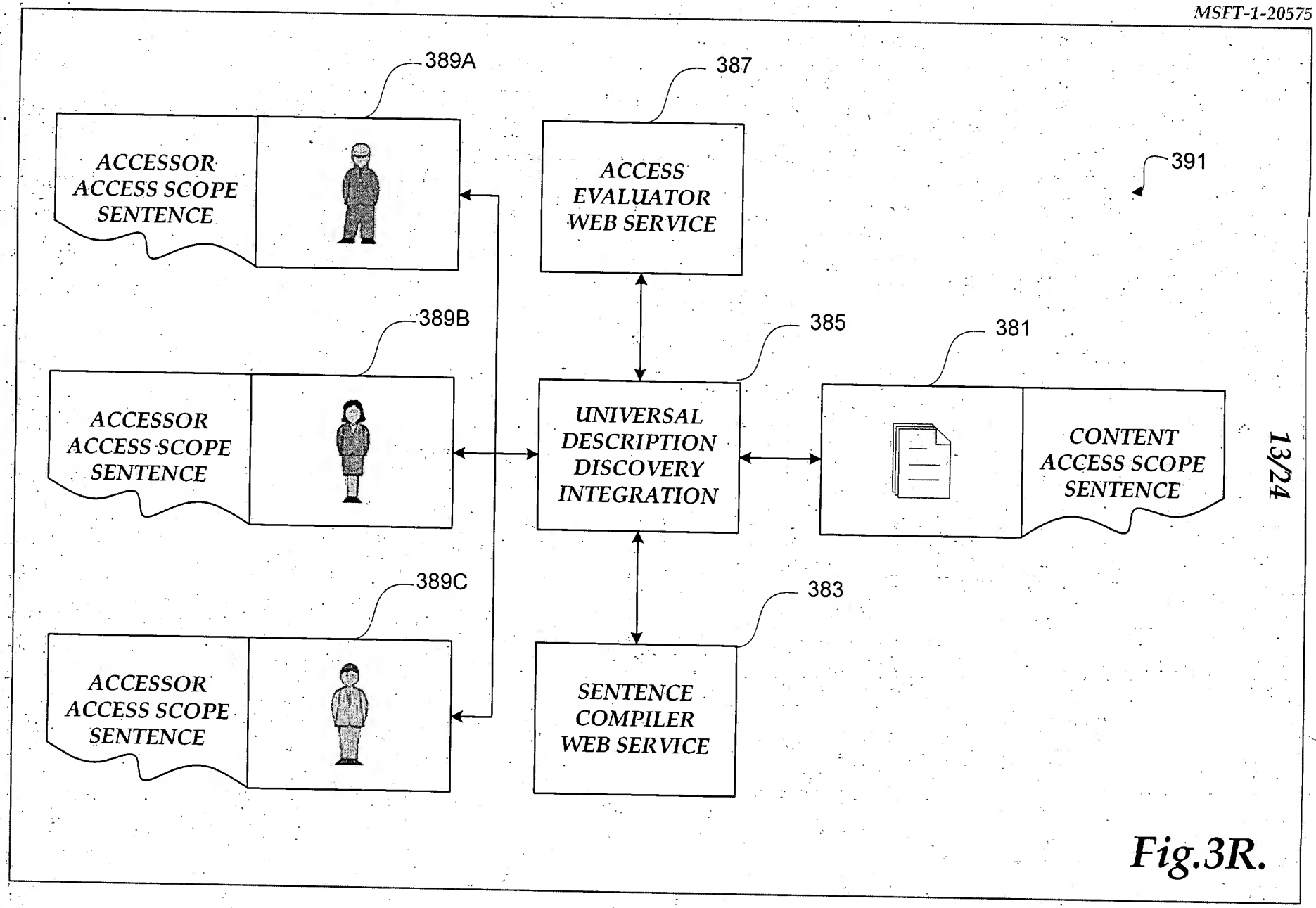


Fig.3Q.



Title: DISTRIBUTED EXPRESSION-BASED ACCESS CONTROL
Inventor: Shawn Oberst
Docket No.: MSFT120575



13/24

Fig.3R.

Title: DISTRIBUTED EXPRESSION-BASED ACCESS CONTROL
Inventor: Shawn Oberst
Docket No.: MSFT120575

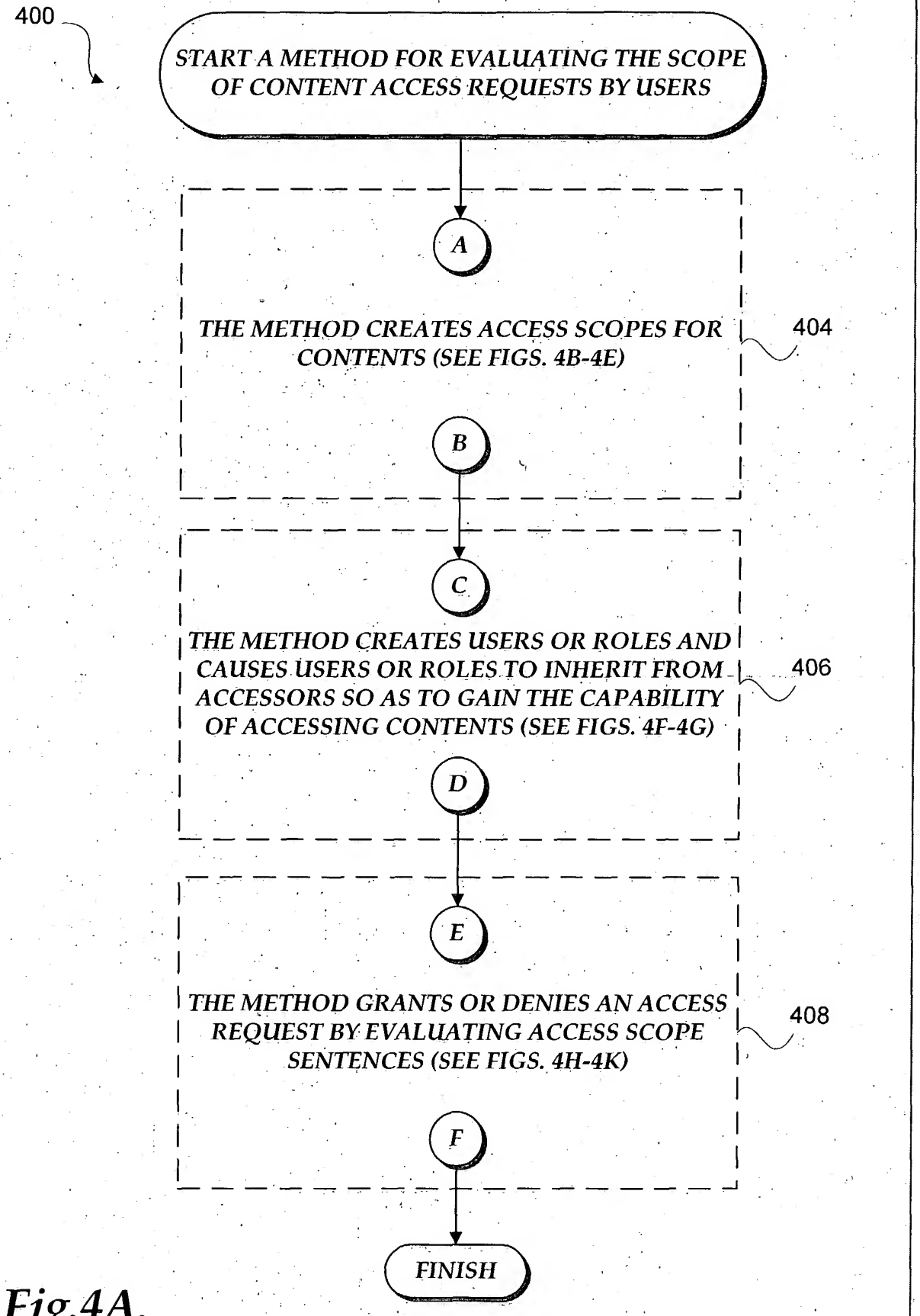
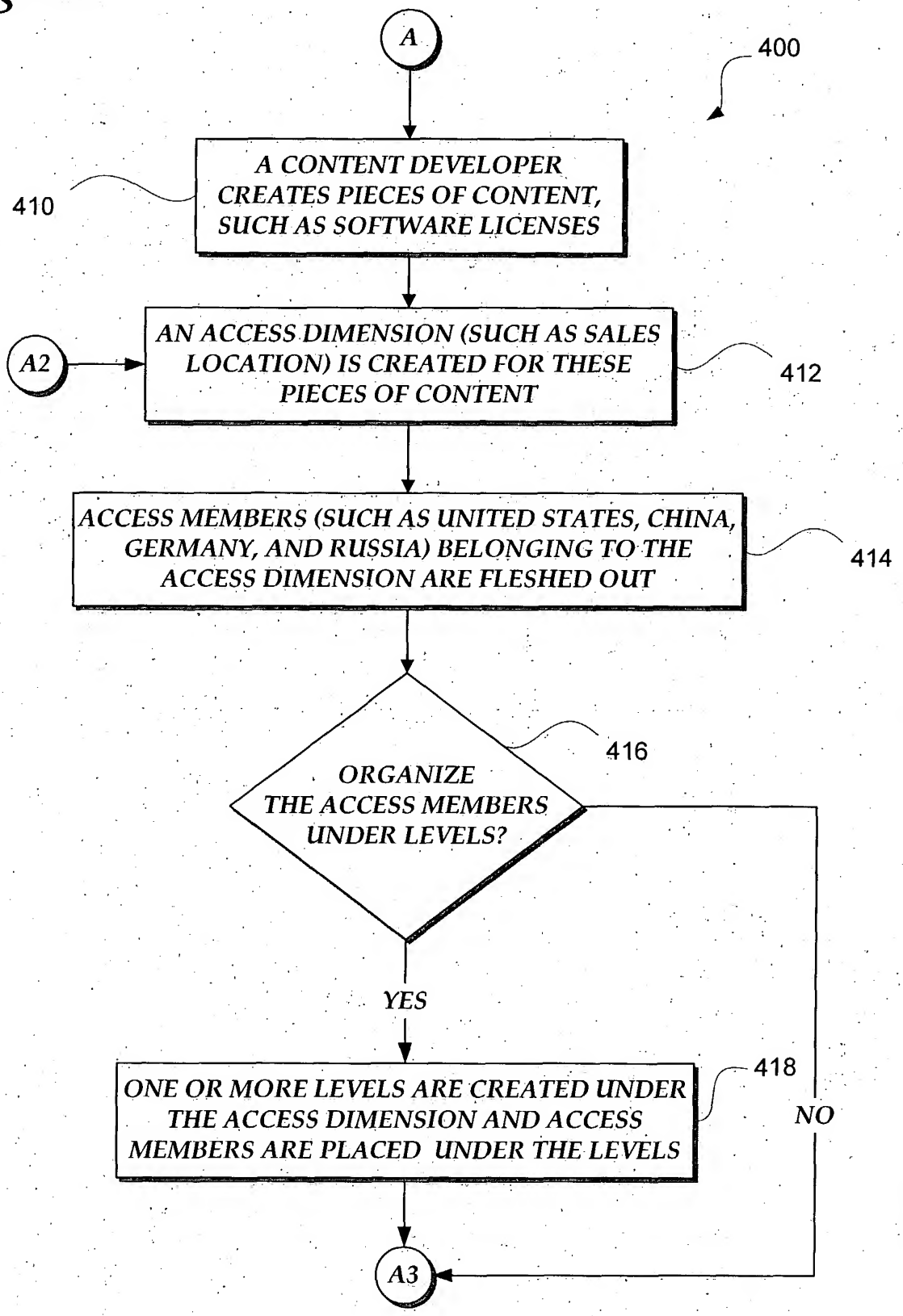

400
START A METHOD FOR EVALUATING THE SCOPE OF CONTENT ACCESS REQUESTS BY USERS
A
THE METHOD CREATES ACCESS SCOPES FOR CONTENTS (SEE FIGS. 4B-4E)
404
B
C
THE METHOD CREATES USERS OR ROLES AND CAUSES USERS OR ROLES TO INHERIT FROM ACCESSORS SO AS TO GAIN THE CAPABILITY OF ACCESSING CONTENTS (SEE FIGS. 4F-4G)
406
D
E
THE METHOD GRANTS OR DENIES AN ACCESS REQUEST BY EVALUATING ACCESS SCOPE SENTENCES (SEE FIGS. 4H-4K)
408
F
FINISH

Fig.4A.

Fig.4B.


A
400
A CONTENT DEVELOPER CREATES PIECES OF CONTENT, SUCH AS SOFTWARE LICENSES
410
A2
AN ACCESS DIMENSION (SUCH AS SALES LOCATION) IS CREATED FOR THESE PIECES OF CONTENT
412
ACCESS MEMBERS (SUCH AS UNITED STATES, CHINA, GERMANY, AND RUSSIA) BELONGING TO THE ACCESS DIMENSION ARE FLESHED OUT
414
ORGANIZE THE ACCESS MEMBERS UNDER LEVELS?
416
YES
ONE OR MORE LEVELS ARE CREATED UNDER THE ACCESS DIMENSION AND ACCESS MEMBERS ARE PLACED UNDER THE LEVELS
418
NO
A3

16/24

Fig.4C.

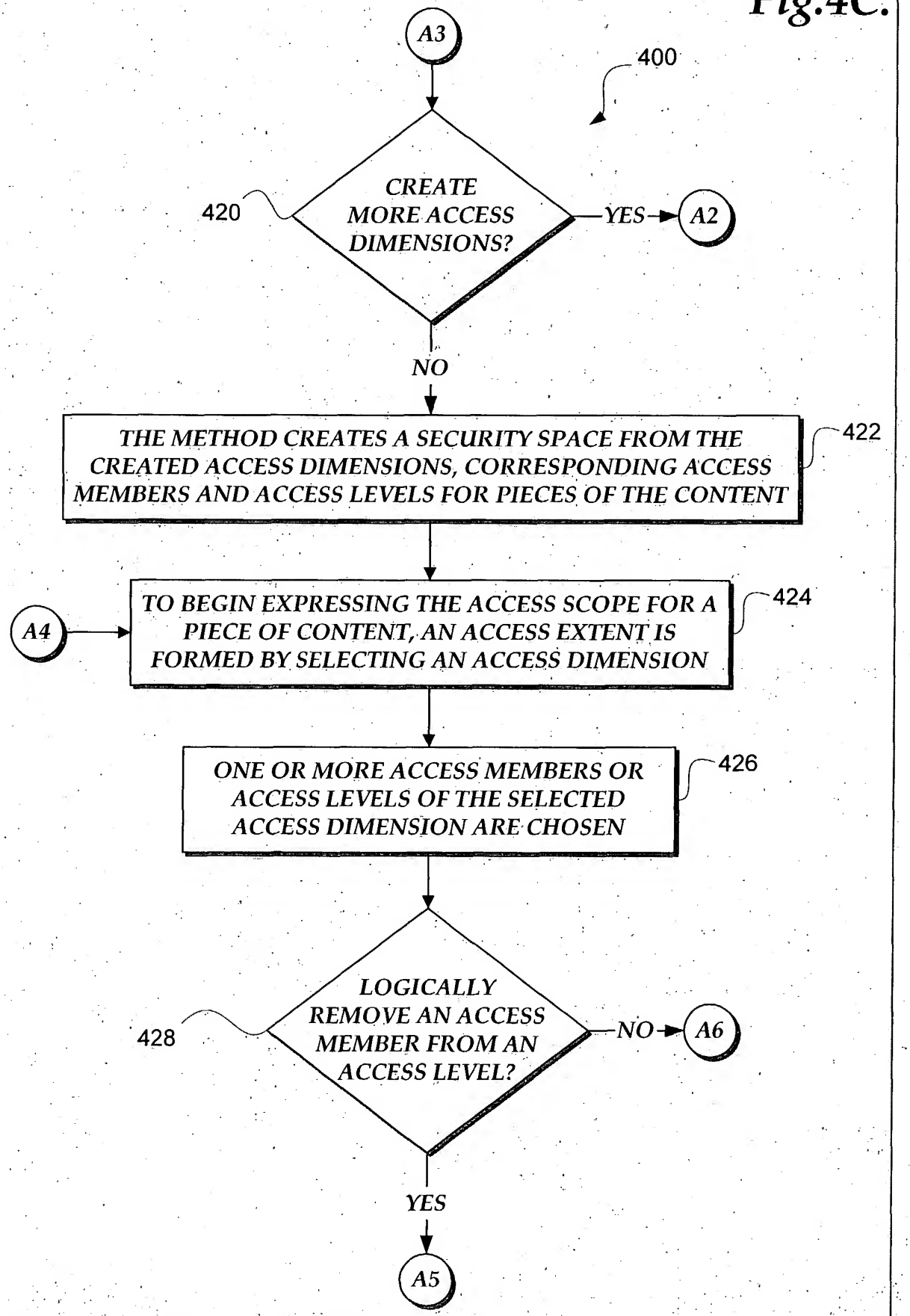

A3
400
CREATE MORE ACCESS DIMENSIONS?
420
YES
A2
NO
THE METHOD CREATES A SECURITY SPACE FROM THE CREATED ACCESS DIMENSIONS, CORRESPONDING ACCESS MEMBERS AND ACCESS LEVELS FOR PIECES OF THE CONTENT
422
A4
TO BEGIN EXPRESSING THE ACCESS SCOPE FOR A PIECE OF CONTENT, AN ACCESS EXTENT IS FORMED BY SELECTING AN ACCESS DIMENSION
424
ONE OR MORE ACCESS MEMBERS OR ACCESS LEVELS OF THE SELECTED ACCESS DIMENSION ARE CHOSEN
426
LOGICALLY REMOVE AN ACCESS MEMBER FROM AN ACCESS LEVEL?
428
NO
A6
YES
A5

Fig.4D.

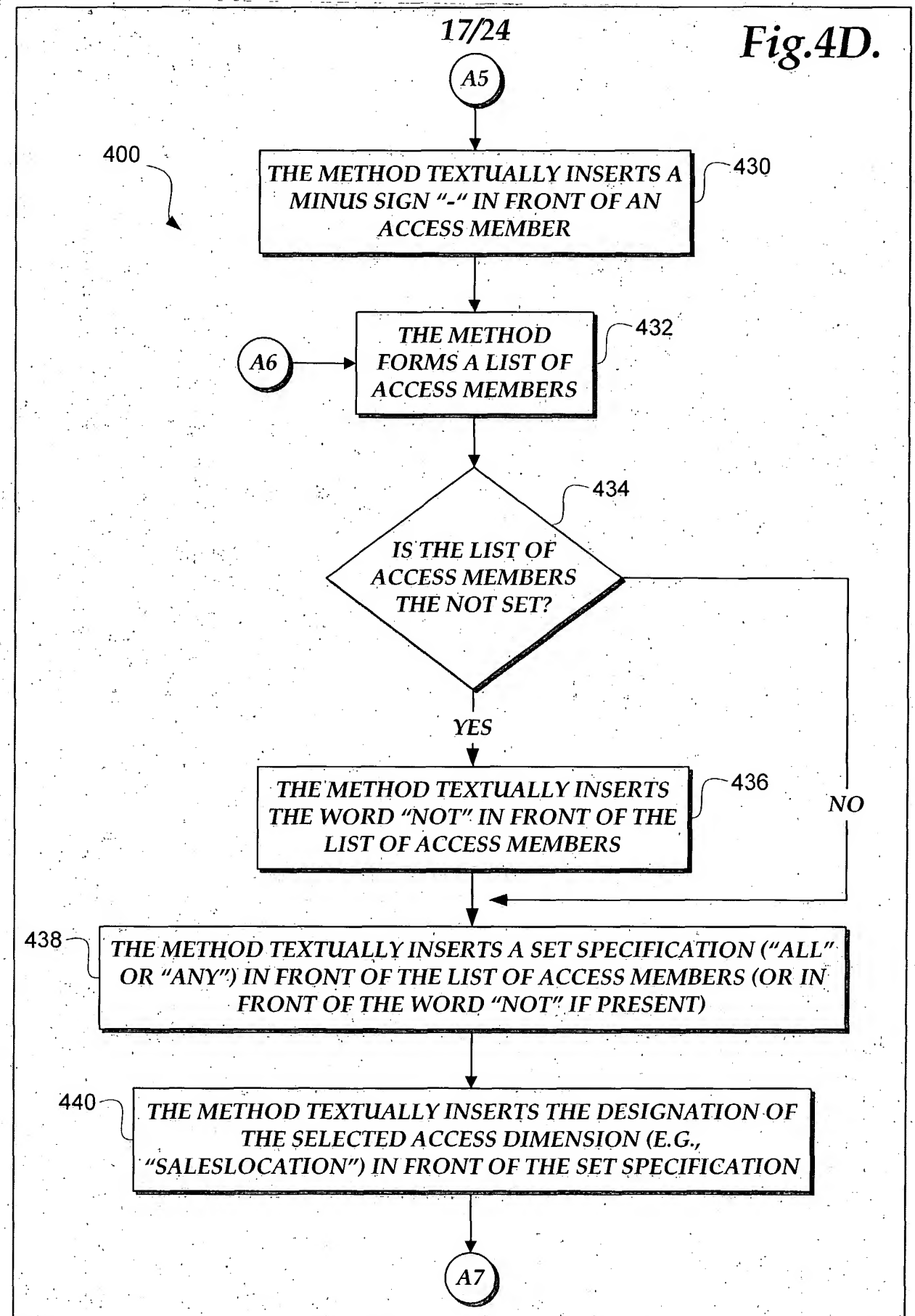

A5
400
THE METHOD TEXTUALLY INSERTS A MINUS SIGN "-" IN FRONT OF AN ACCESS MEMBER
430
A6
THE METHOD FORMS A LIST OF ACCESS MEMBERS
432
IS THE LIST OF ACCESS MEMBERS THE NOT SET?
434
YES
NO
THE METHOD TEXTUALLY INSERTS THE WORD "NOT" IN FRONT OF THE LIST OF ACCESS MEMBERS
436
438
THE METHOD TEXTUALLY INSERTS A SET SPECIFICATION ("ALL" OR "ANY") IN FRONT OF THE LIST OF ACCESS MEMBERS (OR IN FRONT OF THE WORD "NOT" IF PRESENT)
440
THE METHOD TEXTUALLY INSERTS THE DESIGNATION OF THE SELECTED ACCESS DIMENSION (E.G., "SALESLOCATION") IN FRONT OF THE SET SPECIFICATION
A7

Fig.4E.

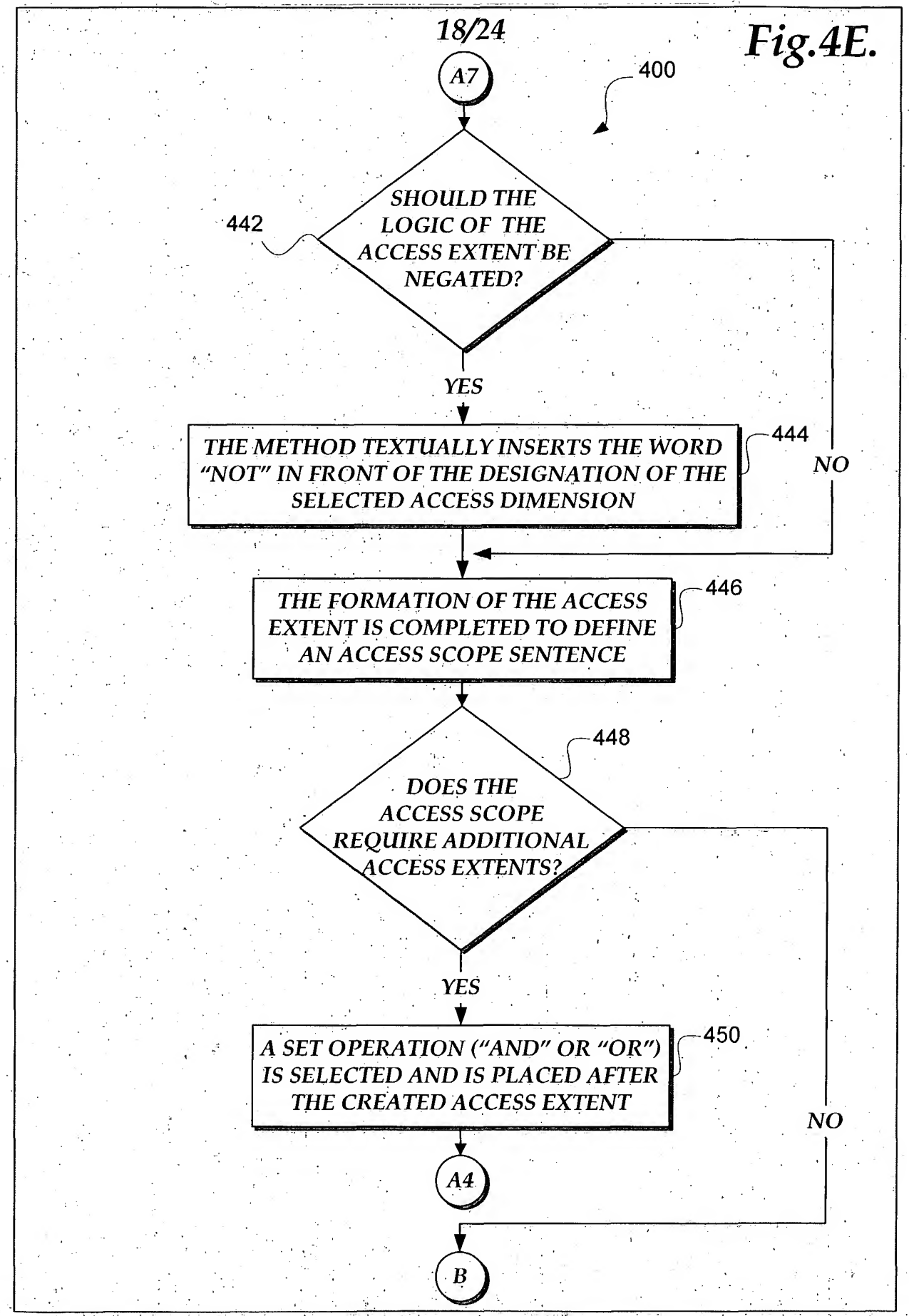

A7
400
SHOULD THE LOGIC OF THE ACCESS EXTENT BE NEGATED?
442
YES
NO
THE METHOD TEXTUALLY INSERTS THE WORD "NOT" IN FRONT OF THE DESIGNATION OF THE SELECTED ACCESS DIMENSION
444
THE FORMATION OF THE ACCESS EXTENT IS COMPLETED TO DEFINE AN ACCESS SCOPE SENTENCE
446
DOES THE ACCESS SCOPE REQUIRE ADDITIONAL ACCESS EXTENTS?
448
YES
NO
A SET OPERATION ("AND" OR "OR") IS SELECTED AND IS PLACED AFTER THE CREATED ACCESS EXTENT
450
A4
B

Fig.4F.

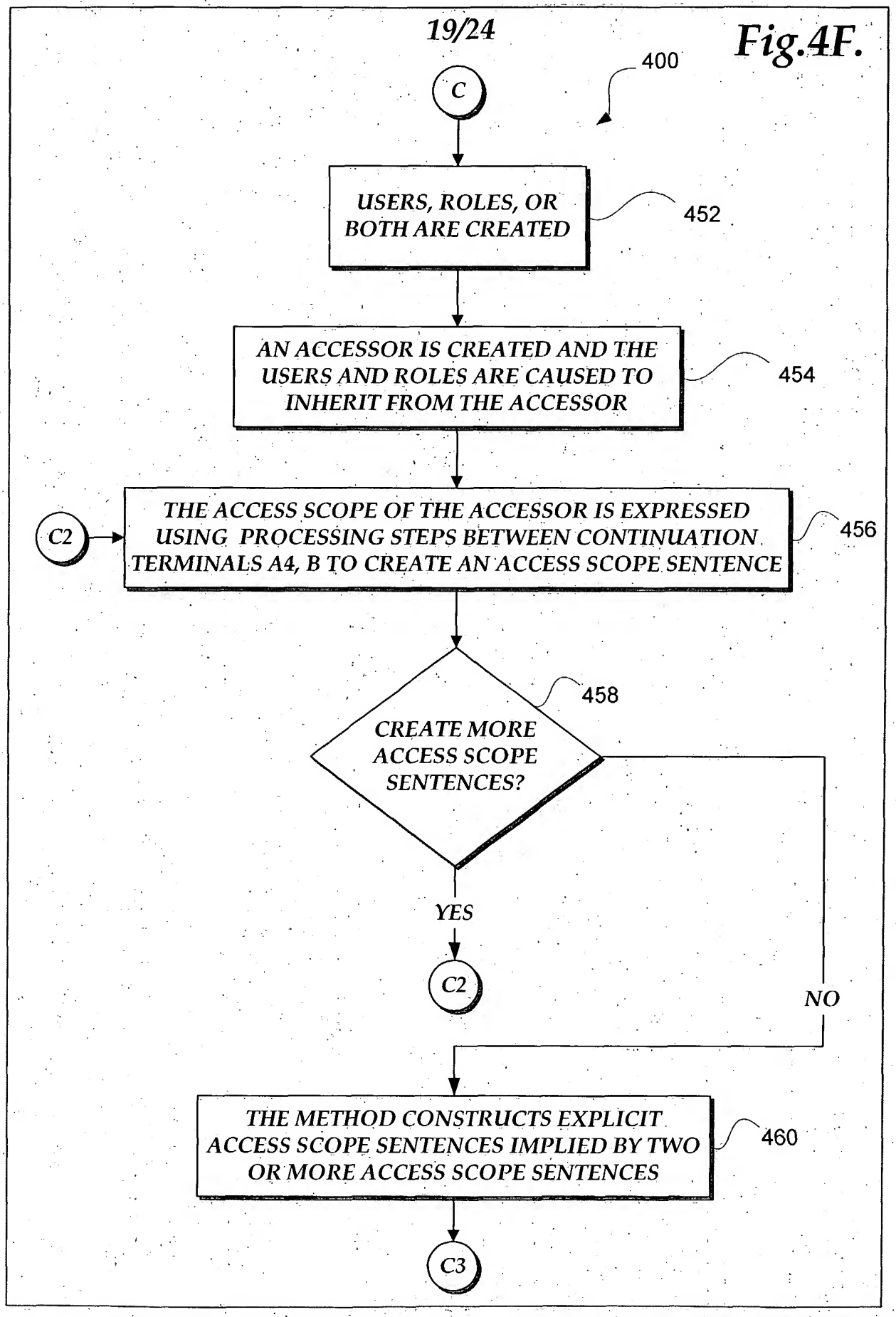

400
C
USERS, ROLES, OR BOTH ARE CREATED
452
AN ACCESSOR IS CREATED AND THE USERS AND ROLES ARE CAUSED TO INHERIT FROM THE ACCESSOR
454
C2
THE ACCESS SCOPE OF THE ACCESSOR IS EXPRESSED USING PROCESSING STEPS BETWEEN CONTINUATION TERMINALS A4, B TO CREATE AN ACCESS SCOPE SENTENCE
456
458
CREATE MORE ACCESS SCOPE SENTENCES?
YES
C2
NO
THE METHOD CONSTRUCTS EXPLICIT ACCESS SCOPE SENTENCES IMPLIED BY TWO OR MORE ACCESS SCOPE SENTENCES
460
C3

Fig.4G.

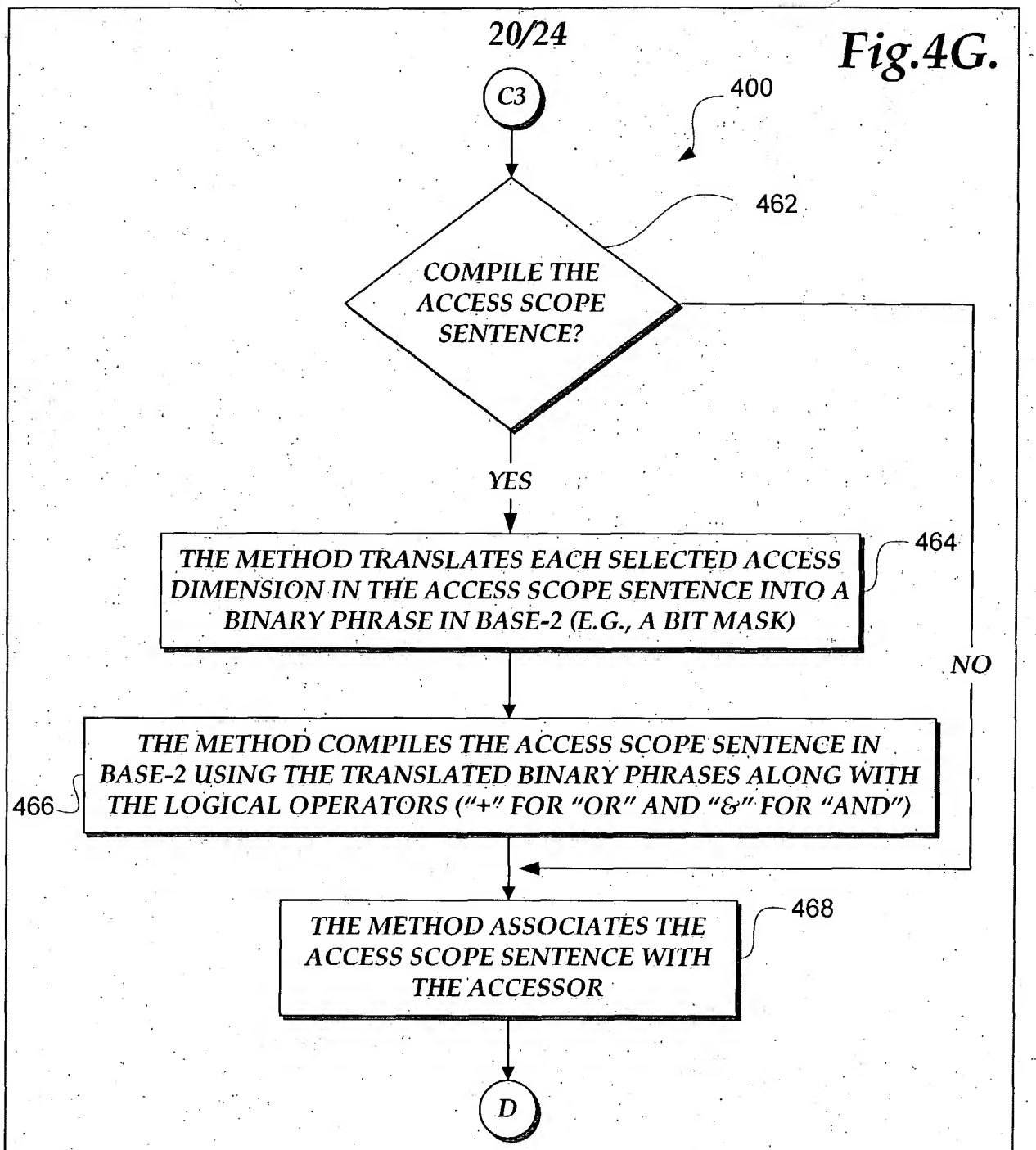

C3
400
462
COMPILE THE ACCESS SCOPE SENTENCE?
YES
NO
464
THE METHOD TRANSLATES EACH SELECTED ACCESS DIMENSION IN THE ACCESS SCOPE SENTENCE INTO A BINARY PHRASE IN BASE-2 (E.G., A BIT MASK)
466
THE METHOD COMPILES THE ACCESS SCOPE SENTENCE IN BASE-2 USING THE TRANSLATED BINARY PHRASES ALONG WITH THE LOGICAL OPERATORS ("+" FOR "OR" AND "&" FOR "AND")
468
THE METHOD ASSOCIATES THE ACCESS SCOPE SENTENCE WITH THE ACCESSOR
D

Fig.4H.

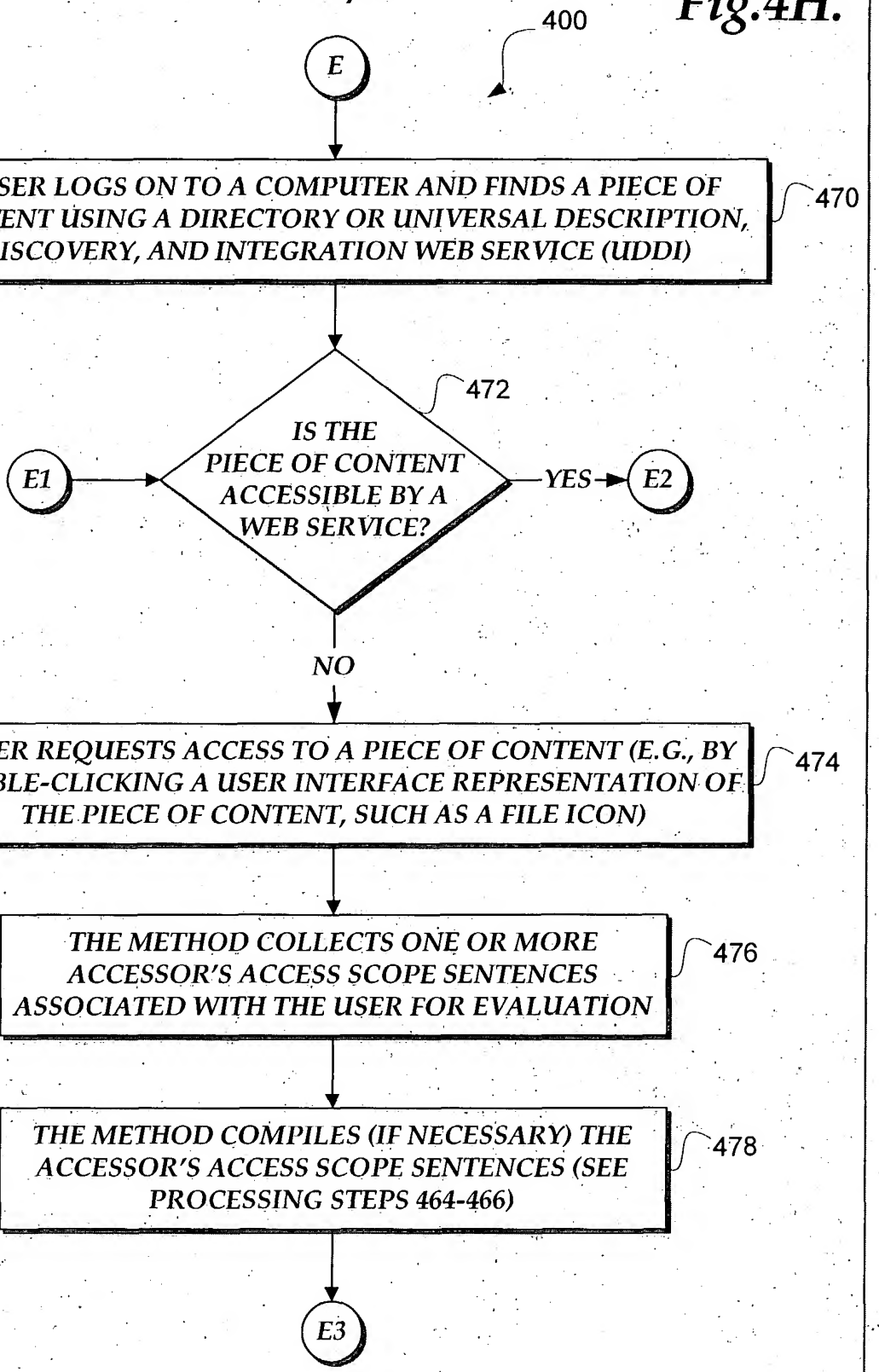

400
E
A USER LOGS ON TO A COMPUTER AND FINDS A PIECE OF CONTENT USING A DIRECTORY OR UNIVERSAL DESCRIPTION, DISCOVERY, AND INTEGRATION WEB SERVICE (UDDI)
470
472
IS THE PIECE OF CONTENT ACCESSIBLE BY A WEB SERVICE?
E1
YES
E2
NO
A USER REQUESTS ACCESS TO A PIECE OF CONTENT (E.G., BY DOUBLE-CLICKING A USER INTERFACE REPRESENTATION OF THE PIECE OF CONTENT, SUCH AS A FILE ICON)
474
THE METHOD COLLECTS ONE OR MORE ACCESSOR'S ACCESS SCOPE SENTENCES ASSOCIATED WITH THE USER FOR EVALUATION
476
THE METHOD COMPILES (IF NECESSARY) THE ACCESSOR'S ACCESS SCOPE SENTENCES (SEE PROCESSING STEPS 464-466)
478
E3

Fig.4I.

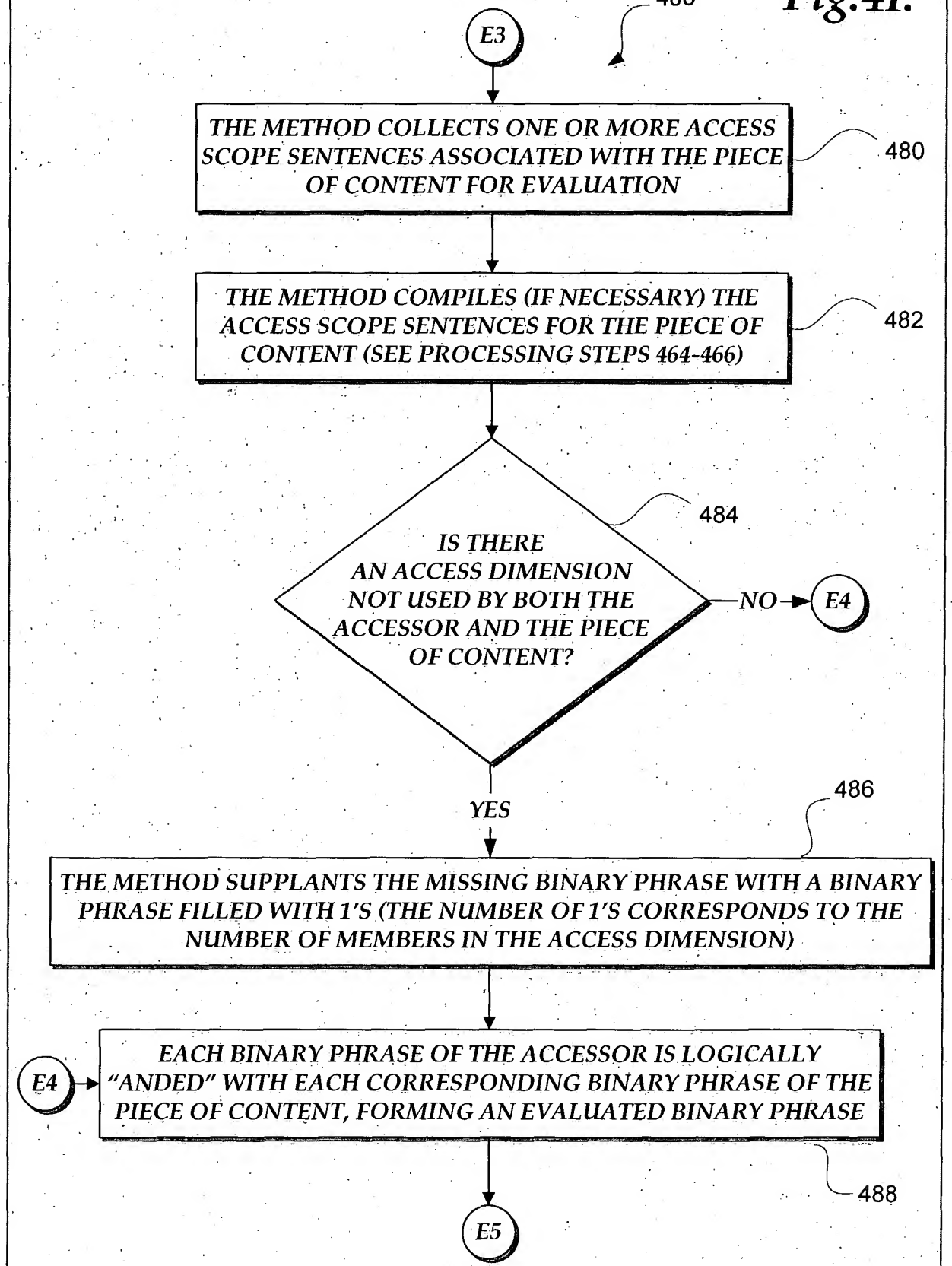

400
E3
THE METHOD COLLECTS ONE OR MORE ACCESS SCOPE SENTENCES ASSOCIATED WITH THE PIECE OF CONTENT FOR EVALUATION
480
THE METHOD COMPILES (IF NECESSARY) THE ACCESS SCOPE SENTENCES FOR THE PIECE OF CONTENT (SEE PROCESSING STEPS 464-466)
482
484
IS THERE AN ACCESS DIMENSION NOT USED BY BOTH THE ACCESSOR AND THE PIECE OF CONTENT?
NO
E4
YES
486
THE METHOD SUPPLANTS THE MISSING BINARY PHRASE WITH A BINARY PHRASE FILLED WITH 1'S (THE NUMBER OF 1'S CORRESPONDS TO THE NUMBER OF MEMBERS IN THE ACCESS DIMENSION)
E4
EACH BINARY PHRASE OF THE ACCESSOR IS LOGICALLY "ANDED" WITH EACH CORRESPONDING BINARY PHRASE OF THE PIECE OF CONTENT, FORMING AN EVALUATED BINARY PHRASE
488
E5

Fig.4J.

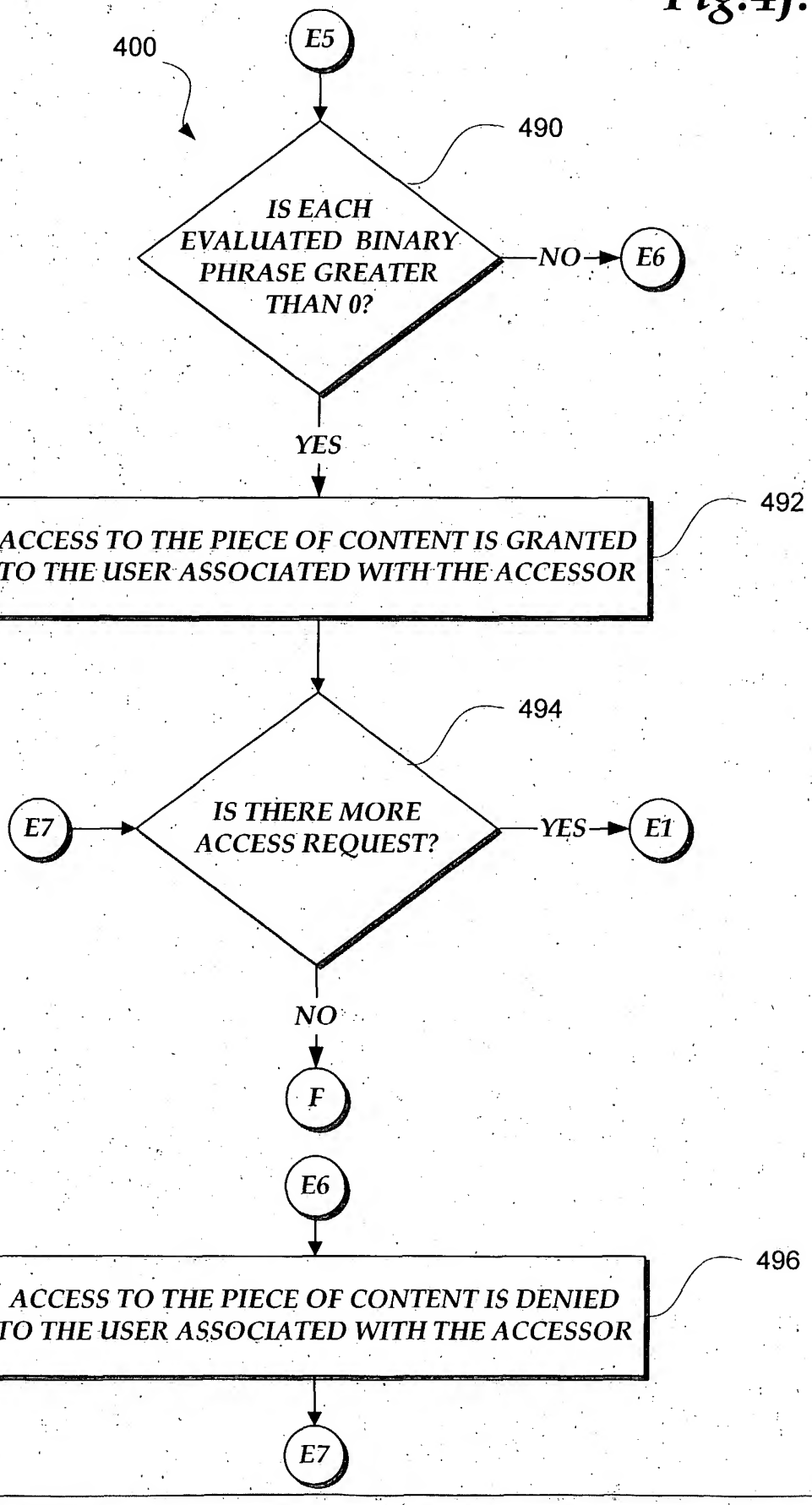
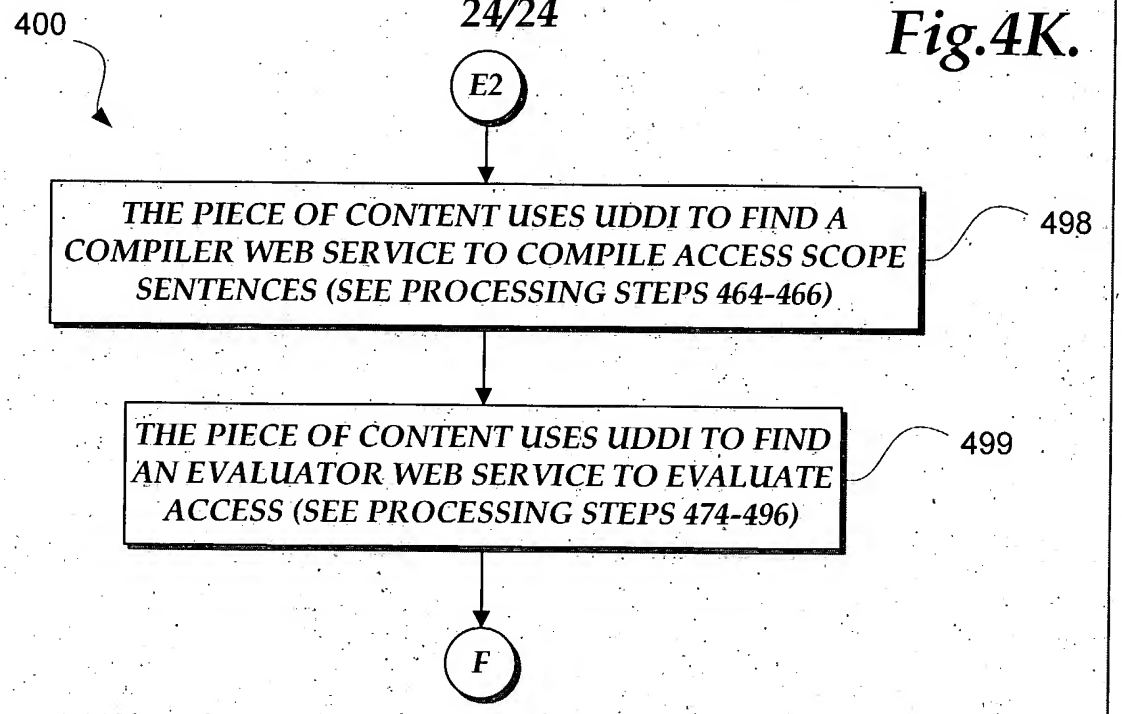

400
E5
490
IS EACH EVALUATED BINARY PHRASE GREATER THAN 0?
NO
E6
YES
492
ACCESS TO THE PIECE OF CONTENT IS GRANTED TO THE USER ASSOCIATED WITH THE ACCESSOR
494
E7
IS THERE MORE ACCESS REQUEST?
YES
E1
NO
F
E6
496
ACCESS TO THE PIECE OF CONTENT IS DENIED TO THE USER ASSOCIATED WITH THE ACCESSOR
E7

Fig.4K.


400
E2
THE PIECE OF CONTENT USES UDDI TO FIND A COMPILER WEB SERVICE TO COMPILE ACCESS SCOPE SENTENCES (SEE PROCESSING STEPS 464-466)
498
THE PIECE OF CONTENT USES UDDI TO FIND AN EVALUATOR WEB SERVICE TO EVALUATE ACCESS (SEE PROCESSING STEPS 474-496)
499
F